

Paul W. HODGSON
Serial No. 10/522,919
February 23, 2010

REMARKS

Reconsideration of this application is respectfully requested. Currently, claims 1-10, 12-18, 20, 22-31 and 33-37 are pending in this application.

Rejection under 35 U.S.C. §103:

Claims 1-4, 8-10, 12-15, 22-24, 31-34 and 36 have been rejected under 35 U.S.C. §103 as allegedly being unpatentable over Paul et al. (U.S. '709, hereinafter "Paul") in view of Steiger et al. (U.S. '097, hereinafter "Steiger"). Claims 11, 19, 21 and 35 have been rejected under 35 U.S.C. §103 as allegedly being unpatentable over Paul in view of Steiger and further in view of Tarbotton et al. (U.S. '830, hereinafter "Tarbotton"). Applicant traverses this rejection.

In order to establish a *prima facie* case of obviousness, all of the claim limitations must be taught or suggested by the prior art. Each of the above-noted combinations fails to teach or suggest all of the claim limitations. For example, each of the above-noted combinations fails to teach or suggest "generat[ing] or receiv[ing] traffic log data based on at least one traffic characteristic using data derived from the handling of plural electronic messages;....[and] analyz[ing] the traffic log data as a function of a predetermined traffic characteristic criterion corresponding to malicious electronic message traffic to identify electronic messages that satisfy the traffic characteristic criterion, the traffic characteristic criterion including the number of electronic messages from a common user, terminal router or other topological position within a time interval (emphasis added)," as required by independent claim 1 and its dependents. Similar comments apply to independent claims 12, 23, 31 and 36.

Paul W. HODGSON
Serial No. 10/522,919
February 23, 2010

With respect to the above-noted claim limitations, page 20 of the Office Action admits “The modified Paul et al. fails to teach that criteria includes an electronic message type or number of electronic messages emanating from a user (emphasis added).” Pages 13-14 of the Office Action appear to make similar admissions. Neither Steiger nor Tarbotton resolves this admitted deficiency.

Page 14-16 and 20-21 of the Office Action apparently allege that col. 8, lines 15-18 of Tarbotton discloses the traffic characteristic criterion including the number of electronic messages from a common user, terminal router or other topological position within a time interval. Applicant respectfully disagrees with this allegation.

Col. 8, lines 15-18 (and following text) of Tarbotton discloses the following:

FIG. 5 illustrates characteristics of a number of example received e-mail messages and how the rules of FIG. 4 may produce a minimum delay period for each message.

In the first example, the received e-mail message includes data indicating

In the second example, the default delay of ten minutes set by rule #1 is increased to six hours by rule #4 on detection of the program.exe attachment....

In the third example, the sender is detected by rule #2 as being internal to the organisation....

The fourth example illustrates how rule #3 detects an e-mail message received from a specific trusted sender....

The fifth example illustrates the application of rule #5 to impose a one hour delay due to detection of a document type attachment to an e-mail

Finally, the sixth example illustrates how rule #7 detects that the message content type of the received e-mail message is html

Paul W. HODGSON
Serial No. 10/522,919
February 23, 2010

The recitation of “characteristics of a number of example received e-mail messages” in the above-reproduced passage of Tarbotton does not disclose the traffic characteristic criterion including the number of electronic messages from a common user, terminal router or other topological position within a time interval, as apparently alleged by the Office Action. Instead, “characteristics of a number of example received e-mail messages” in the above-reproduced passage of Tarbotton merely means that there are a plurality (i.e., “a number”) of different examples of received email messages described below (i.e., “first” through “sixth examples), and that these different examples of email messages have respective characteristics.

The traffic log data recited by independent claim 1 is generated or received based on an at least one traffic characteristic using data derived from the handling of plural electronic messages. Instead, Tarbotton’s first through sixth examples in column 8, lines 15-18 each involves applying rules to a message itself. That is, analysis is performed on the message itself in order to determine a delay, rather than being based on data derived from the handling of plural electronic messages as claimed, let alone using the number of electronic messages from a common user, terminal router or other topological position within a time interval as a traffic characteristic criterion.

Claim 20 has been rejected under 35 U.S.C. §103 as allegedly being unpatentable over Paul in view of Steiger and further in view of Nielson et al. (U.S. ‘327, hereinafter “Nielson”). Applicant traverses this rejection.

Claim 20 requires, among other things, “receiving traffic log data defining at least one message traffic characteristic using data derived from the handling of plural electronic messages

Paul W. HODGSON
Serial No. 10/522,919
February 23, 2010

and emanating from a user relating to electronic messages sent by a user; [and] analyzing the received traffic log data as a function of a specified traffic characteristic criterion corresponding to malicious electronic message traffic to identify those electronic messages that satisfy the criterion, the traffic characteristic criterion including the number of electronic messages from a common user, terminal router or other topological position of the organization within a time interval.” For reasons similar to those discussed above with respect to claim 1, Paul fails to teach or suggest this limitation. Neither Steiger nor Nielson resolves this deficiency.

Claims 5-7 and 16-18 have been rejected under 35 U.S.C. §103 as allegedly being unpatentable over Paul in view of Steiger and further in view of Toyoshima et al. (U.S. ‘349, hereinafter “Toyoshima”). Claims 25-30 have been rejected under 35 U.S.C. §103 as allegedly being unpatentable over Paul in view of Steiger and further in view of Khanna et al. (U.S. ‘604, hereinafter “Khanna”). Applicant traverses these rejections. Claims 5-7 depend at least indirectly from base independent claim 1, claims 16-18 depend at least indirectly from base independent claim 12, and claims 25-30 depend at least indirectly from base independent claim 23. The above comments with respect to these base independent claims thus apply to claims 5-7, 16-18 and 25-30. Neither Toyoshima nor Khanna resolve these deficiencies.

New claim:

New claim 37 has been added. New claim 37 requires, *inter alia*, “the traffic characteristic criterion including the volume of data passing at a point along a data path or link in a time interval encompassing a plurality of electronic messages.” Applicant thus submits that new claim 37 is allowable.

Paul W. HODGSON
Serial No. 10/522,919
February 23, 2010

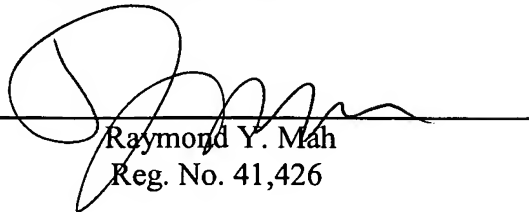
Conclusion:

Accordingly, this entire application is now believed to be in condition for allowance, and a formal notice to that effect is earnestly solicited.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: _____


Raymond Y. Mah
Reg. No. 41,426

RYM:dmw
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100